TRUTH11.COM

Pilot CBDC Shows Central Bank Has Total Control • Freeze User Accounts, Decrease Targeted Addresses Balances, Arrest, And Mint New Units Of The Digital Currency (CBDC)

Dylan Eleven
Aug 2, 2023 4 min

The Expose | Patricia Harrity

The pilot project of Brazil’s Central Bank Digital Currency the Real Digital allows the freezing of user wallets and reducing balances, as was always highly suspected by “conspiracy theorists!”

The Real Digital

The president of the Central Bank, Roberto Campos Neto, presented Brazil’s digital agenda back in November 2022 where a preview of the Real Digital app was presented. According to Campos “The Real Digital, the central bank digital currency (CBDC) in Brazil, appears to tokenize the banking system” he explained that the “CBDC is nothing more than a token issued by the bank upon deposit” (source).

However, it is clearly more than that as revealed in a report by Journalist Vini Barbosa on the website Portal do Bitcoin.

The Public Audit

On Monday the 3rd of July the Central Bank of Brazil (Bacen) published information on their Central Bank Digital Currency Pilot scheme which offered public participation in its audit. As a result, developers found that the digital currency allows the freezing and manipulation of users’ wallets.

According to Barbosa, following the publication of the documentation about the Brazilian CBDC pilot project on GitHub, the Central Bank of Brazil also allowed the start of a public audit of the system’s source code.

The public and collaborative audit of their pilot CBDC on the open platform “Kit Onboarding” contains documentation and configuration files that can be accessed by anyone as one of the purposes of publishing the pilot, (as written in the project’s so-called “Onboarding Kit”), is to receive feedback — leaving all documentation subject to evolution or changes.

Developers

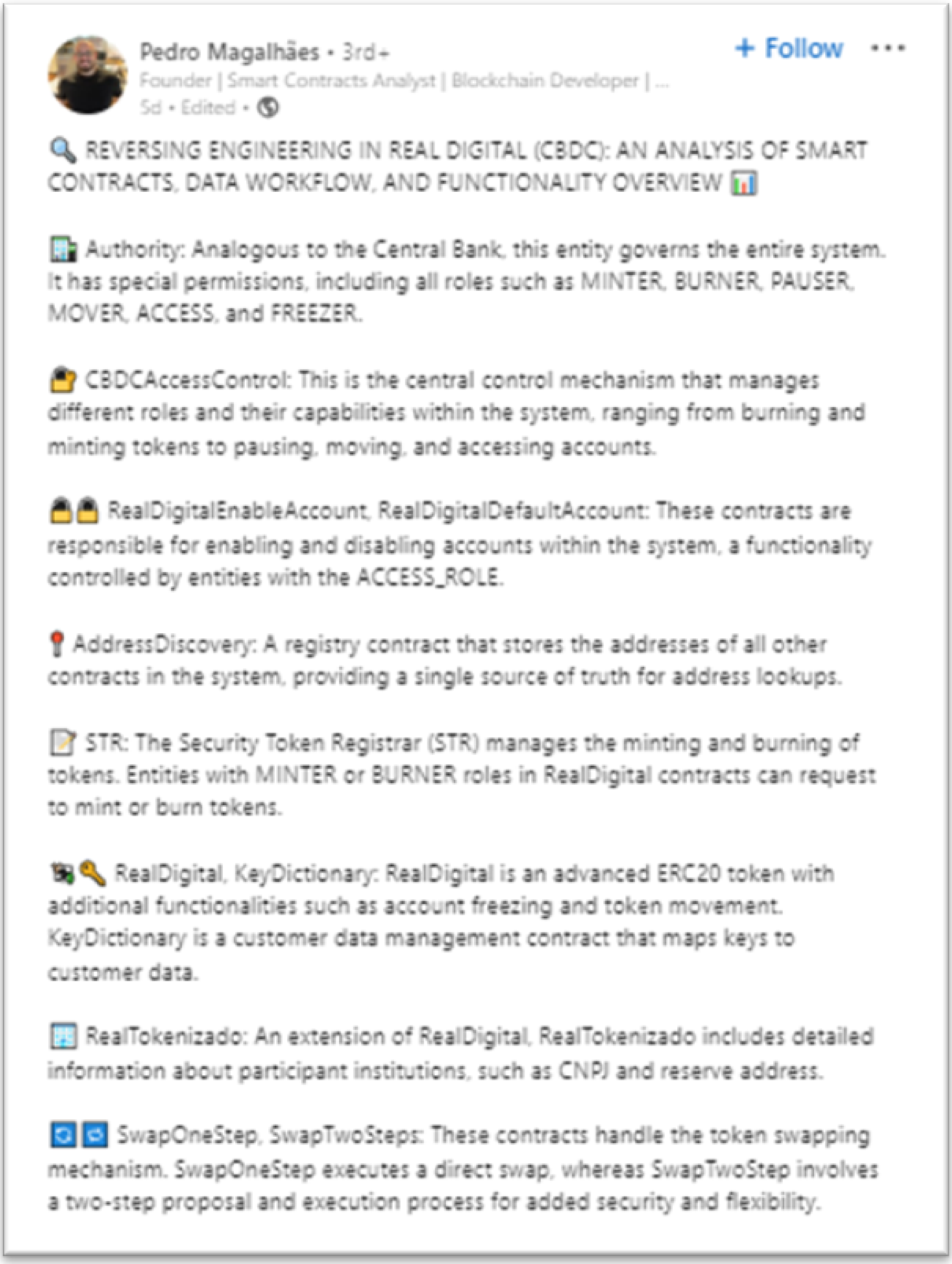
As we would expect, the audit attracted attention and feedback from a number of developers who went on to analyse the code leading to the discovery of a few unknown code functions (Commands). These functions essentially allow the controllers to make several relevant changes in the data of the CBDCs ledger, directly affecting its users.

Reverse Engineering

One full-stack developer Pedro Magalhães who specialises in Blockchain and DeFI, and the programming language Solidity, announced on LinkedIn that he had “discovered Solidity’s Source Code of the CBDC through the ABI (interface) of Real Digital using reverse engineering”.

Magalhães wrote “Recently, I delved into the world of ABIs (interfaces) of Real Digital, a Central Bank’s initiative, with the intention of exploring possible vulnerabilities for purely didactic purposes.”

In a conversation with **Portal do Bitcoin**, Magalhães explained “Reverse engineering is a technique to understand how a system works just by observing its behaviour” and that an Application Binary Interface (ABI) is “basically a way to interact with smart contracts on Ethereum.



Pedro Magalhães • 3rd+
Founder | Smart Contracts Analyst | Blockchain Developer | ...
5d • Edited •

🔍 REVERSING ENGINEERING IN REAL DIGITAL (CBDC): AN ANALYSIS OF SMART CONTRACTS, DATA WORKFLOW, AND FUNCTIONALITY OVERVIEW 📊

🏦 Authority: Analogous to the Central Bank, this entity governs the entire system. It has special permissions, including all roles such as MINTER, BURNER, PAUSER, MOVER, ACCESS, and FREEZER.

🔐 CBDCAccessControl: This is the central control mechanism that manages different roles and their capabilities within the system, ranging from burning and minting tokens to pausing, moving, and accessing accounts.

🔒🔒 RealDigitalEnableAccount, RealDigitalDefaultAccount: These contracts are responsible for enabling and disabling accounts within the system, a functionality controlled by entities with the ACCESS_ROLE.

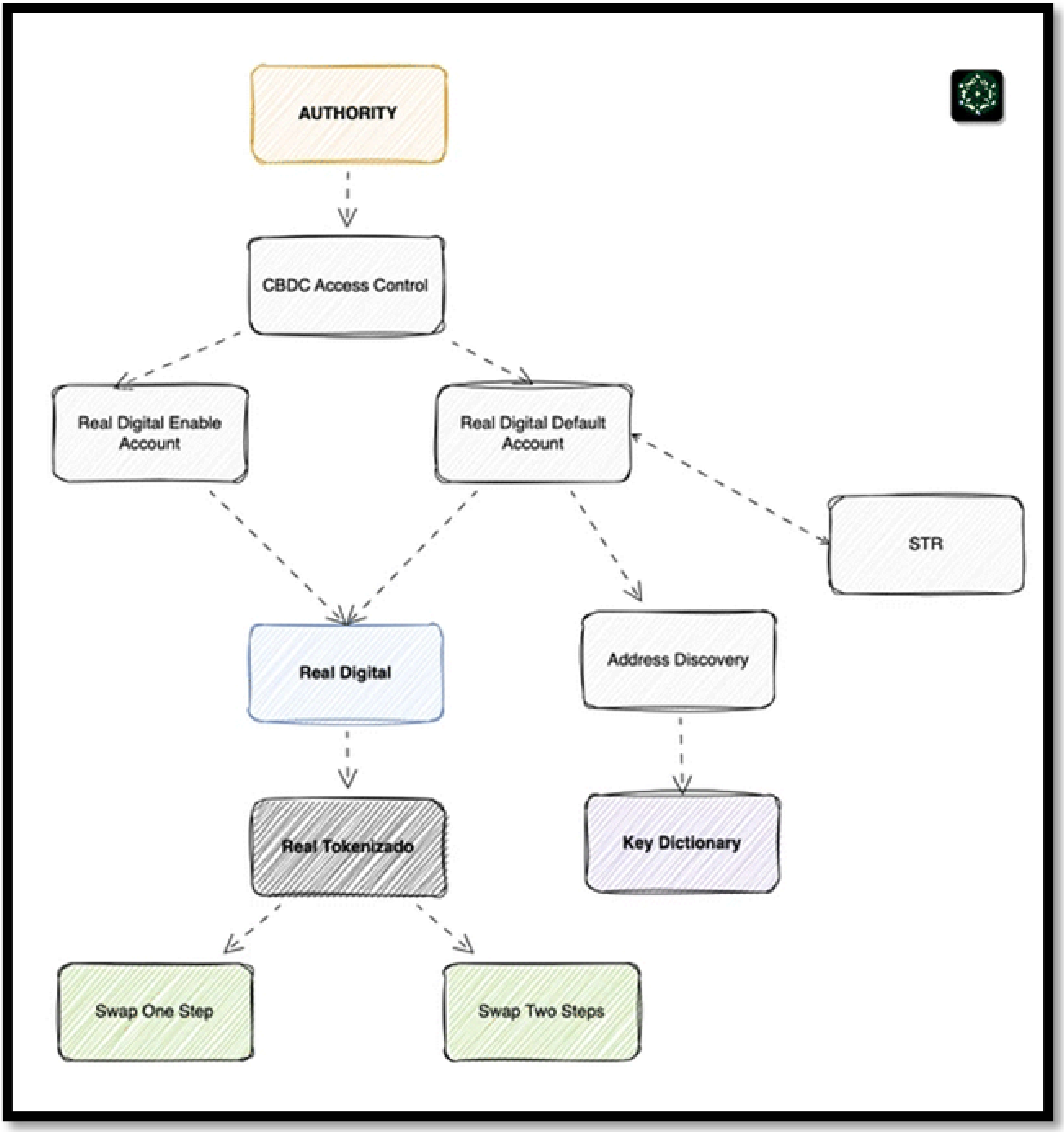
📍 AddressDiscovery: A registry contract that stores the addresses of all other contracts in the system, providing a single source of truth for address lookups.

📝 STR: The Security Token Registrar (STR) manages the minting and burning of tokens. Entities with MINTER or BURNER roles in RealDigital contracts can request to mint or burn tokens.

💸🔑 RealDigital, KeyDictionary: RealDigital is an advanced ERC20 token with additional functionalities such as account freezing and token movement. KeyDictionary is a customer data management contract that maps keys to customer data.

🏢 RealTokenizado: An extension of RealDigital, RealTokenizado includes detailed information about participant institutions, such as CNPJ and reserve address.

🔄🔃 SwapOneStep, SwapTwoSteps: These contracts handle the token swapping mechanism. SwapOneStep executes a direct swap, whereas SwapTwoStep involves a two-step proposal and execution process for added security and flexibility.



It is like a manual that tells how the contract can be read and written.” He explains, continuing, “I analysed the ABI to understand Real Digital’s functionalities and discovered the various functions they implemented.”

This led to his many findings including operations such as “minting” Real Digital tokens and enabling/disabling target accounts. Also, through applying the reverse engineering technique, he was able to find functions that can be executed by any entity that receives proper permissions from the controlling entity of the new system — i.e., the Central Bank.

Based on this analysis, Pedro says it was possible to recreate the smart contract in Solidity (the computing language) used in the pilot project. This contract enables the execution of the following functions:

disableAccount: Disables an account authorized to transfer tokens.

enableAccount: Enables an account previously disabled for token transfers.

increaseFrozenBalance: Increases the frozen balance of a wallet address.

decreaseFrozenBalance: Decreases the frozen balance of a wallet address.

transfer: Overrides the ERC20 transfer function to include account status checks and frozen balances.

transferFrom: Overrides the ERC20 transferFrom function to include account status checks and frozen balances.

mint: Creates new Real Digital tokens for a specified address.

burn: Burns (destroys) a specified amount of Real Digital tokens.

pause: Pauses token transfers.

unpause: Resumes token transfers.

frozenBalanceOf: Retrieves the frozen balance of a wallet address.

authorizedAccount: Checks if an account is authorized for token transfers.

move: Transfer tokens from one wallet to another.

moveAndBurn: Transfers and burns tokens from a wallet.

burnFrom: Burns tokens from a specified account.

These functions can be performed by any entity authorized by the Central Bank through another function (also present in the source code), called *Access Control*. **Portal do Bitcoin** also checked and confirmed with other developers the existence of these functions in the **Real Digital** source code.

Intended For Test Environment?

Barbosa says, that the Brazilian Bank originally stated that “the **Real Digital** pilot project is intended for use only in a test environment and should not be reproduced for real operations.” However, when asked by the report, the Central Bank admitted the possibility of executing the functions discovered by Magalhães.

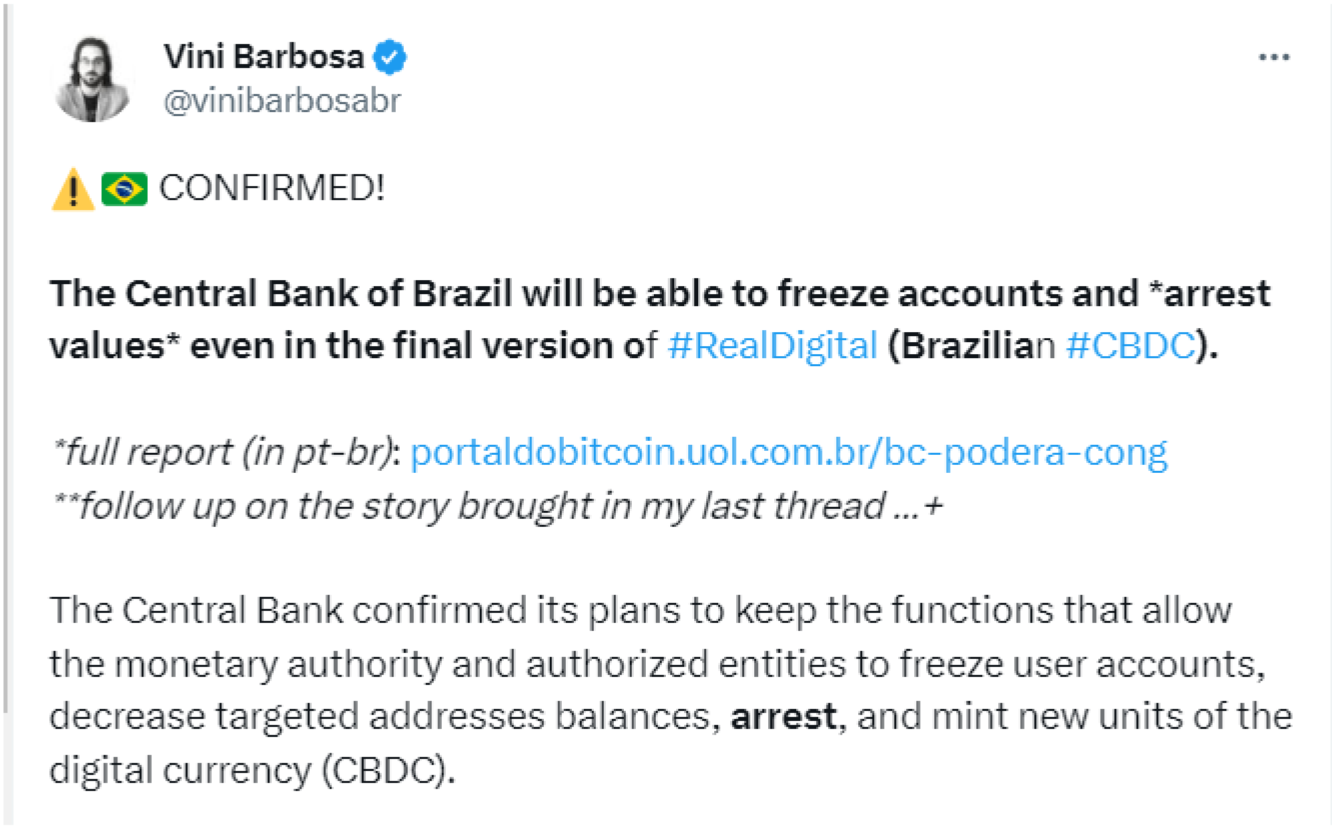
However, “The BC and institutions already have similar functionalities in the current environment of systems such as SPB and Pix, their use being governed by law and regulation”, informed the country’s monetary authority.

The Bank Confirmed It Is Keeping The Functions

The Central Bank confirmed its plans to keep the functions that allow the monetary authority and authorized entities to freeze user accounts, decrease targeted addresses balances, **arrest**, and mint new units of the digital currency (CBDC).

Barbosa Tweeted “Until today, the population was only speculating if they would be kept after the **Real Digital**‘s official launch; or if they were only made for the test network.

**full report (in pt-br)*: https://portaldobitcoin.uol.com.br/bc-podera-cong



Vini Barbosa
@vinibarbosabr

⚠️🇧🇷 CONFIRMED!

The Central Bank of Brazil will be able to freeze accounts and *arrest values* even in the final version of #RealDigital **(Brazilia**n #CBDC**).**

*full report (in pt-br): portaldobitcoin.uol.com.br/bc-podera-cong
**follow up on the story brought in my last thread ...+

The Central Bank confirmed its plans to keep the functions that allow the monetary authority and authorized entities to freeze user accounts, decrease targeted addresses balances, **arrest**, and mint new units of the digital currency (CBDC).

This ability to “freeze or arrest amounts” held in this System is protected by current legislation in Brazil, according to the Central Bank. Did we really expect anything else? Why would they give up those functions that make it easier for them to control the masses?

Image: Source

Original Article: https://expose-news.com/2023/07/31/pilot-cbdc-shows-central-bank-has-total-control/